UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/664,069 | 09/16/2003 | Chch Goh | B-5236 621255-8 | 3247 |

7590 01/16/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

| EXAMINER | |
|---|---|
| HA, LEYNNA A | |
| ART UNIT | PAPER NUMBER |
| 2135 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 01/16/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/664,069 | GOH ET AL. | |
| | Examiner | Art Unit | |
| | LEYNNA T. HA | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) 1-40 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-40 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

**1.** Claims 1-40 is pending.

### *Information Disclosure Statement*

**2. The information disclosure statement filed 9/16/2003 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because** the IDS does not seem to apply for this current application. The IDS contains the wrong attorney docket number and different inventor name than in the oath of declaration submitted with this application. **It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).**

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**3. Claims 1-40 are rejected under 35 U.S.C. 102(e) as being anticipate by Schneck, et al. (US 6,314,409).**

**As per claim 1:**

Schneck discloses a system comprising: an output device for outputting data onto a removable storage medium:

a first computing entity arranged to encrypt a first data set based on encryption parameters comprising public data of a trusted party and an encryption key string **(col.13, lines 31-39; the claimed public data can broadly be given as Schneck's ancillary information such as identification or unencrypted data that does not need protection. The encrypted ancillary information is the first data set that comprises the public data (col.10, lines 49-53).)** comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium **(col.11, line 55 – col.12, line 8**

**and col.14, lines 11-16; Schneck discloses a variety of removable storage mediums (col.15, lines 10-23) in the form of packages, vendor software packages, CD-ROM, cards, etc. The second data set is in the form of access rules that defines a policy that is packaged data (col.13, lines 24-28).)**, the first computing entity being further arranged to output the encrypted first data set for the output device; and **(col.15, lines 50-59; Schneck discloses a variety of output devices in the forms of display, printer, modem, network connection devices, etc.)**

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data; **(col.8, lines 8-18 and col.17, lines 35-40)**

the output device being arranged to use the decryption key in decrypting the encrypted first data set. **(col.22, lines 8-15 and col.26, lines 57-67)**

**As per claim 2: See col.22, lines 8-15 and col.26, lines 65-67);** discusses a system according to claim 1, wherein the second computing entity is arranged to generate the decryption key only when said policy has been met.

**As per claim 3: See col.7, lines 5-6 and col.27, lines 11-20;**

discusses a system according to claim 1, wherein the second computing entity is arranged to issue to the first computing entity at least one of: the second data set; the encryption key string; a derivative of the encryption key string usable by the first computing entity, in place of the encryption key string, in the encryption of said first data set.

**As per claim 4: See col.17, lines 8-13 and col.26, lines 57-66;** discusses a system according to claim 1, wherein the second computing entity is arranged to receive the encryption key string directly or indirectly from the first computing entity.

**As per claim 5: See col.17, lines 8-40 and col.26, lines 57-66;** discusses a system according to claim 1, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising for the or each said further trusted party the public data of that trusted party and a respective further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set; the or each further second computing entity being arranged, when satisfied that the policy defined by the encryption key string related to the associated trusted party has been met, to provide a further decryption key to the output device, the second computing entity concerned being arranged to generate this further decryption key in dependence on the private data and encryption key string corresponding to the associated trusted party; and decryption

of the encrypted first data set by the output device requiring use of the decryption keys provided by all of the trusted parties.

**As per claim 6: See col.19, line 58 – col.20, line 3 and col.23, lines 1-16;** discusses a system according to claim 5, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the output device is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the output device.

**As per claim 7: See col.23, lines 1-16 and col.26, lines 57-67;** discusses a system according to claim 5, wherein the first computing entity is arranged to process the first data set, prior to encryption, to form a plurality of data strings, the first computing entity being further arranged to encrypt each data string based on the encryption parameters associated with a respective one of the trusted parties, and the output device being arranged to decrypt each string using the decryption key provided by the related trusted party and then to process the strings to recover the first data set.

**As per claim 8: See col.22, lines 8-15 and col.26, lines 57-67;**

discusses a system according to claim 1, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising the public data of the or each further trusted party; each second computing entity being arranged, when satisfied that the policy defined by the encryption key string has been met so far as the associated trusted party is concerned, to provide a respective decryption key to the output device, the second computing entity concerned being arranged to generate this decryption key in dependence on the encryption key string and the private data of the associated trusted party; and decryption of the encrypted first data set by the output device requiring use of the decryption keys provided by all of the trusted parties.

**As per claim 9: See col.22, lines 8-15 and col.23, lines 1-16;** discusses a system according to claim 8, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each second computing entity being arranged to be satisfied that said policy has been met when the set of at least one condition for the trusted party associated with the second computing entity concerned has been met.

**As per claim 10: See col.19, line 58 – col.20, line 3 and col.22, lines 8-15;** discusses a system according to claim 8, wherein the first data set concerns a document to be published, the first computing entity and one

of the second computing entities are both associated with a document publisher, and the output device is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the output device.

**As per claim 11: See col.12, lines 33-35 and 47-50;** discusses a system according to claim 1, wherein the first data set is encrypted using a bilinear pairing technique.

**As per claim 12: See col.12, lines 33-35 and 47-50;** discusses a system according to claim 1, wherein the first data set is encrypted using a quadratic residue technique.

**As per claim 13: See col.15, lines 50-59;** discusses a system according to claim 1, wherein the output device and the second computing entity are incorporated into the same item of equipment.

**As per claim 14: See col.15, lines 18-23 and 50-59;** discusses a system according to claim 1, further comprising a portable device comprising the second computing entity and a first communications interface, the output device comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the

output device; the communications interfaces being such that the portable device must be present at the output device for the communication between the second computing entity to take place.

**As per claim 15:**

Schneck discloses a data output method comprising the steps of:

(a) encrypting a first data set based on encryption parameters comprising public data of a trusted party and an encryption key string **(col.13, lines 31-39; the claimed public data can broadly be given as Schneck's ancillary information such as identification or unencrypted data that does not need protection. The encrypted ancillary information is the first data set that comprises the public data (col.10, lines 49-53).)** comprising a second data set that defines a policy for allowing the output of the first data set to a removable storage medium, **(col.11, line 55 – col.12, line 8 and col.14, lines 11-16; Schneck discloses a variety of removable storage mediums (col.15, lines 10-23) in the form of packages, vendor software packages, CD-ROM, cards, etc. The second data set is in the form of access rules that defines a policy that is packaged data (col.13, lines 24-28).)**

(b) providing the encrypted first data set to an output device adapted to output data to a removable storage medium; **(col.15, lines 50-59; Schneck discloses a variety of output devices in the forms of display, printer, modem, network connection devices, etc.)**

(c) at the trusted party checking that said policy has been satisfied and thereafter providing the output device with a decryption key for use in decrypting the encrypted first data set, this decryption key being generated in dependence on the encryption key string and private data related to said public data; and **(col.8, lines 8-18 and col.17, lines 35-40)**

(d) at the output device using the decryption key in decrypting the encrypted first data set and outputting the first data set to a removable recording medium. **(col.22, lines 8-15 and col.26, lines 65-67)**

**As per claim 16: See col.22, lines 8-15 and col.26, lines 65-67);** discusses a method according to claim 15, wherein in step (c) the decryption key is generated only after said policy has been satisfied.

**As per claim 17: See col.7, lines 5-6 and col.27, lines 11-20;** discusses a method according to claim 15, further comprising an initial step of generating the second data set at the trusted party and providing to a party that is to carry out step (a) at least one of: the second data set; the encryption key string; a derivative of the encryption key string usable in step (a), in place of the encryption key string, in the encryption of said first data set.

**As per claim 18: See col.17, lines 8-13 and col.26, lines 57-66;** discusses a method according to claim 15, wherein the trusted party receives the encryption key string directly or indirectly from a party that carries out step (a).

**As per claim 19: See col.17, lines 8-40 and col.26, lines 57-66;** discusses a method according to claim 15, wherein: in step (a) said encryption parameters further comprise public data of at least one further trusted party and a respective related further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set; in step (c) the or each further trusted party, when satisfied that the policy defined by the related encryption key string has been met, provides a further decryption key to the output device, the further trusted party concerned generating this further decryption key in dependence on private data and said related encryption key string; and in step (d) decryption of the encrypted first data set by the output device requires use of the decryption keys provided by all of the trusted parties.

**As per claim 20: See col.19, line 58 – col.20, line 3 and col.23, lines 1-16;** discusses a method according to claim 19, wherein: the first data set concerns a document to be published; step (a) is carried out by a document publisher who also serves as one of the trusted parties; the output device is associated with a document seller; in step (c) the trusted party associated with the document publisher checks satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and in step (c) another of said trusted parties checks satisfaction of at least one condition concerning the output device.

**As per claim 21: See col.23, lines 1-16 and col.26, lines 57-67;** discusses a method according to claim 19, wherein: in step (a) the first data set is processed, prior to encryption, to form a plurality of data strings, each string being thereafter encrypted based on the encryption parameters associated with a respective one of the trusted parties, and in step (d) the output device decrypts each string using the decryption key provided by the related trusted party and then processes the strings to recover the first data set.

**As per claim 22: See col.22, lines 8-15 and col.26, lines 57-67;** discusses a method according to claim 15, wherein: in step (a) said encryption parameters further comprise public data of at least one further trusted party; in step (c) each trusted party, when satisfied that the policy defined by the encryption key string has been met so far as it is concerned, provides a respective decryption key to the output device, the further trusted party concerned generating this decryption key in dependence on private data and the encryption key string; and in step (d) decryption of the encrypted first data set by the output device requires use of the decryption keys provided by all of the trusted parties.

**As per claim 23: See col.22, lines 8-15 and col.23, lines 1-16;** discusses a method according to claim 22, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each trusted party being arranged to be satisfied that said policy has been met when the set of at least one condition associated

with the trusted party has been met.

**As per claim 24: See col.19, line 58 – col.20, line 3 and col.22, lines 8-15;** discusses a method according to claim 22, wherein: the first data set concerns a document to be published; step (a) is carried out by a document publisher who also serves as one of the trusted parties; the output device is associated with a document seller; in step (c) the trusted party associated with the document publisher checks satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and in step (c) another of said trusted parties checks satisfaction of at least one condition concerning the output device.

**As per claim 25: See col.12, lines 33-35 and 47-50;** discusses a method according to claim 15, wherein in step (a) the first data set is encrypted using a bilinear pairing technique.

**As per claim 26: See col.12, lines 33-35 and 47-50;** discusses a method according to claim 15, wherein in step (a) the first data set is encrypted using a quadratic residue technique.

**As per claim 27: See col.15, lines 18-23 and 50-59;** discusses a method according to claim 15 wherein the trusted authority is implemented in a portable device arranged to communicate with the output device only when the portable device is present at the output device.

**As per claim 28:**

Schneck discloses a printing system comprising: a printer;

a first computing entity arranged to encrypt a first data set based on encryption parameters comprising public data of a trusted party and an encryption key string **(col.13, lines 31-39; the claimed public data can broadly be given as Schneck's ancillary information such as identification or unencrypted data that does not need protection. The encrypted ancillary information is the first data set that comprises the public data (col.10, lines 49-53).)** comprising a second data set that defines a policy for allowing the printing of the first data set, the first computing entity being further arranged to output the encrypted first data set for the printer; and **(col.11, line 55 – col.12, line 8 and col.14, lines 11-16; Schneck discloses a variety of removable storage mediums (col.15, lines 10-23) in the form of packages, vendor software packages, CD-ROM, cards, etc. The second data set is in the form of access rules that defines a policy that is packaged data (col.13, lines 24-28).)**,

a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the printer **(col.15, lines 50-59; Schneck discloses a variety of output devices in the forms of display, printer, modem, network connection devices, etc.)** a decryption key for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private

data related to said public data; **(col.8, lines 8-18 and col.17, lines 35-40)**

the printer being arranged to use the decryption key in decrypting the encrypted first data set. **(col.22, lines 8-15 and col.26, lines 65-67)**

**As per claim 29: See col.17, lines 8-40 and col.26, lines 57-66;** discusses a system according to claim 28, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising for the or each said further trusted party the public data of that trusted party and a respective further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set; the or each further second computing entity being arranged, when satisfied that the policy defined by the encryption key string related to the associated trusted party has been met, to provide a further decryption key to the printer, the second computing entity concerned being arranged to generate this further decryption key in dependence on the private data and encryption key string corresponding to the associated trusted party; and decryption of the encrypted first data set by the printer requiring use of the decryption keys provided by all of the trusted parties.

**As per claim 30: See col.19, line 58 – col.20, line 3 and col.23, lines 1-16;** discusses a system according to claim 29, wherein the first data set concerns a document to be published, the first computing entity and

one of the second computing entities are both associated with a document publisher, and the printer is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the printer.

**As per claim 31: See col.23, lines 1-16 and col.26, lines 57-67;** discusses a system according to claim 29, wherein the first computing entity is arranged to process the first data set, prior to encryption, to form a plurality of data strings, the first computing entity being further arranged to encrypt each data string based on the encryption parameters associated with a respective one of the trusted parties, and the printer being arranged to decrypt each string using the decryption key provided by the related trusted party and then to process the strings to recover the first data set.

**As per claim 32: See col.22, lines 8-15 and col.26, lines 57-67;** discusses a system according to claim 28, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising the public data of the or each further trusted party; each second computing entity being arranged, when

satisfied that the policy defined by the encryption key string has been met so far as the associated trusted party is concerned, to provide a respective decryption key to the printer, the second computing entity concerned being arranged to generate this decryption key in dependence on the encryption key string and the private data of the associated trusted party; and decryption of the encrypted first data set by the printer requiring use of the decryption keys provided by all of the trusted parties.

**As per claim 33: See col.22, lines 8-15 and col.23, lines 1-16;** discusses a system according to claim 32, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each second computing entity being arranged to be satisfied that said policy has been met when the set of at least one condition for the trusted party associated with the second computing entity concerned has been met.

**As per claim 34: See col.19, line 58 – col.20, line 3 and col.22, lines 8-15;** discusses a system according to claim 32, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the printer is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to

the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the printer.

**As per claim 35: See col.12, lines 33-35 and 47-50;** discusses a system according to claim 28, wherein the first data set is encrypted using a bilinear pairing technique.

**As per claim 36: See col.12, lines 33-35 and 47-50;** discusses a system according to claim 28, wherein the first data set is encrypted using a quadratic residue technique.

**As per claim 37: See col.15, lines 50-59;** discusses a system according to claim 28, wherein the printer and the second computing entity are incorporated into the same item of equipment.

**As per claim 38: See col.15, lines 18-23 and 50-59;** discusses a system according to claim 28, further comprising a portable device comprising the second computing entity and a first communications interface, the printer comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the printer; the communications interfaces being such that the portable device must be present at the printer for the communication between the second computing entity to take place.

**As per claim 39:**

Schneck discloses a printing apparatus including:

means for receiving both an encryption key string comprising policy data **(col.13, lines 24-28; the policy data is in the form of access rules that defines a policy that is packaged dat)**, defining a policy for allowing the printing of payload data, and said payload encrypted based on encryption parameters comprising public data of a trusted party and said encryption key string; **(col.13, lines 31-39; the claimed public data can broadly be given as Schneck's ancillary information such as identification or unencrypted data that does not need protection. The encrypted ancillary information is the first data set that comprises the public data (col.10, lines 49-53).)**

means for providing the encryption key string to the trusted authority and for receiving back a decryption key; and **(col.8, lines 8-18 and col.17, lines 35-40)**

means for using the received decryption key in decrypting the encrypted payload data for printing. **(col.22, lines 8-15 and col.26, lines 65-67)**

**As per claim 40: See col.10, lines 22-25;** discusses an item of equipment comprising printing apparatus according to claim 39, and a computing entity arranged to serve as said trusted party.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100